



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/060,780	01/30/2002	Travis Myron Cossel	10012156-1	8265

7590 01/12/2006

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER
----------

SHAW, YIN CHEN

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 01/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/060,780	COSSEL ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Yin-Chen Shaw	2135	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 October 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

1. This written action is responding to the amendment dated 10/25/2005.
2. Claims 1-9, 11-12, and 14-22 have been amended with Claims 1, 4, 5, 7, 9, 11, 12, 14, 16, 19, 20, and 22 as independent claims.
3. Claims 1-23 have been examined and rejected.
4. Rejections of Independent claims are provided with detailed citations from the prior art.
5. Detailed explanation of the citation from prior art is in Italicized font.

## Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 6, 9, 13, 16, and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Pang et al. (U.S. Patent 6,446,204).

a. Referring to Claims 1 and 16:

As per Claim 1, Pang et al. disclose an authentication system, comprising:

A system for authentication, comprising: a processor circuit having a processor and a memory [Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information. Computer system 100 also includes a main memory 106, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 102 for storing information and instructions to be executed by processor 104 (lines 13-20, Col. 4); *where computer system inherently contains circuit board (mother board) for integrating the processor, memory, and other peripheral devices*];

an authentication system stored in the memory and executable by the processor, [Fig. 6 is a block diagram of a system 600 that provides for an extensible authentication mechanism in a stateless web environment (lines 59-61, Col. 18m, Fig. 6, and Fig 8); *were the web application server 280 in the system 600 is a type software program and must be stored in the memory to be executed by the processor*] the authentication system comprising:

a plurality of authentication agents, each of the authentication agents authenticating at least one user parameter by performing at least one authentication task [A plurality of authentication service providers (simply referred to as providers) (lines 1-2, Col. 19). Each provider

provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair (lines 26-31, Col. 20). A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)]; and

an authentication manager [Authentication engine 602, an authentication host 604 (line 67, Col. 18 and line 1, Col. 19)] that requests each of the authentication agents to authenticate an unauthenticated user parameter until all of the authentication agents

have been requested to authenticate the unauthenticated user parameter and the authenticated user parameter is authenticated by at least one of the authentication agents, unless one of the authentication agents fails to authenticate the unauthenticated user parameter **[It shall be assumed that the URL associated with the browser request is associated with the protected string "BASIC(GRUP1) AND IP(IP\_LIST)" and that the browser request contains a username of JIM, a password of "MANAGER" and an IP address of "192.6.25.3". In addition, it shall be assumed that provider 606 is a BASIC type of provider and that provider 608 is an IP type provider (lines 17-23, Col. 22). At step 714, the authentication host 604 sends the provider requests to the appropriate providers. In this example, the provider request of BASIC(GROUP1) JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608. At step 716, each provider determines whether access to the cartridge should be allowed based on the information contained in the provider request that they received (lines 45-52, Col. 22). At step 720, authentication engine 602 applies any logical operations that were associated with the authentication request. In this example, authentication engine 602 applies the logical operation "AND" to the two response messages that were received from provider 606 and provider 608 (lines 57-61,**

**Col. 22); where in this embodiment Pang et al. disclose all the fields, BASIC(GROUP1)JIM/MANAGER and IP(IP\_LIST)192.6.25.3, are passed to the authentication agents (provider 608 and 608) as per request associated with the protected string. In this embodiment, the overall authentication result would be negative when one of the provider returns a negative (failing) authentication result due to the logical "AND" operation].**

As per Claim 16, it encompasses limitations that are similar to those of Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above. In addition, Pang et al. disclose a computer program embodied on a computer readable medium for performing authentication **[The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 104 for execution (lines 58-60, Col. 4)].**

**b. Referring to Claims 6 and 21:**

As per Claim 6, the rejection of Claim 1 is incorporated. In addition, Pang et al. disclose the system of claim 1, wherein: each of the authentication agents transmits an invalid response to the authentication manager upon a failure to authenticate the unauthenticated user parameter **[(lines 39-42 and 54-57, Col. 20)]; and**

each of the authentication agents transmits a valid response to the authentication manager if the unauthenticated user parameter is successfully authenticated **[(lines 35-39 and 50-54, Col. 20)]**.

As per Claim 21, the rejection of Claim 16 is incorporated. In addition, Claim 21 is a computer readable medium corresponding to the method claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above.

c. Referring to Claim 9:

As per Claim 9, Pang et al. disclose an authentication method, comprising:

executing a plurality of authentication agents in a computer system **[Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information (lines 13-16, Col. 4). Provider are implemented as dynamically linked libraries (DLL) (lines 1-2, Col. 20); *where the provider is software implemented and must be executed by the computer*]**, each of the authentication agents being configured to perform at least one authentication task **[A plurality of authentication service providers (simply referred to as providers) (lines 1-2, Col. 19). Each provider provides a specific authentication function to restrict access to a particular cartridge.**



For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair (lines 26-31, Col. 20). A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)]; and

sequentially requesting each of the authentication agents to authenticate an unauthenticated user parameter input into the computer system [It shall be assumed that the URL associated with the browser request is associated with the protected string "BASIC(GRUP1) AND IP(IP\_LIST)" and that the browser request contains a username of

JIM, a password of "MANAGER" and an IP address of "192.6.25.3" (lines 17-21, Col. 22). At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 45-49, Col. 22); *where provider 606 is authenticating the first field of the request, and the provider 608 is authenticating the second field of the request*] until all of the authentication agents have been requested to authenticate the unauthenticated user parameter and the authenticated user parameter is authenticated by at least one of the authentication agents, unless one of the authentication agents fails to authenticate the unauthenticated user parameter [It shall be assumed that the URL associated with the browser request is associated with the protected string "BASIC(GROUP1) AND IP(IP\_LIST)" and that the browser request contains a username of JIM, a password of "MANAGER" and an IP address of "192.6.25.3". In addition, it shall be assumed that provider 606 is a BASIC type of provider and that provider 608 is an IP type provider (lines 17-23, Col. 22). At step 714, the authentication host 604 sends the provider requests to the appropriate providers. In this example, the provider request of BASIC(GROUP1) JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider

608. At step 716, each provider determines whether access to the cartridge should be allowed based on the information contained in the provider request that they received (lines 45-52, Col. 22). At step 720, authentication engine 602 applies any logical operations that were associated with the authentication request. In this example, authentication engine 602 applies the logical operation "AND" to the two response messages that were received from provider 606 and provider 608 (lines 57-61, Col. 22); *where in this embodiment Pang et al. disclose all the fields, BASIC(GROUP1)JIM/MANAGER and IP(IP\_LIST)192.6.25.3, are passed to the authentication agents (provider 606 and 608) as per request associated with the protected string. In this embodiment, the overall authentication result would be negative when one of the provider returns a negative (failing) authentication result due to the logical "AND" operation].*

d. Referring to Claim 13:

As per Claim 13, the rejection of Claim 9 is incorporated. In addition, Claim 13 encompasses limitations that are similar to those of Claim 6. Thus, it is rejected with the same rationale applied against Claim 6 above.

7. Claims 2, 7-8, 14-15, 17, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pang et al. (U.S. Patent 6,446,204).

a. Referring to Claim 2 and 17:

As per Claim 2, Pang et al. disclose the system of claim 1. In addition, Pang et al. disclose each response indicating whether the unauthenticated user parameter has been authenticated **[The provider then sends a response message back up to the authentication engine 602 via the authentication host 604 and the object request broker 282. The response message indicates whether access should be authorized based on the information contained in that particular provider request (lines 17-22, Col. 19)]**. Pang et al. do not expressly disclose wherein the authentication manager waits for a response from each of the authentication agents. However, Pang et al. disclose the request may be removed from the waiting list and the message may be sent to the browser to indicate that the request cannot be processed if the request stayed on the waiting list for a predetermined amount of time **[If the revised browser request remains on the waiting list for more than a predetermined amount of time, listener 210 may remove the request from the waiting list and send a message to the browser 202 to indicate that the request could not be processed (lines 60-64, Col. 16)]**. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention was

made to modify Pang et al. to have the predetermined-waiting-time feature incorporated into the authentication process since one would have been motivated to increase the efficiency of the application server (line 9, Col. 13 from Pang et al.) by imposing an additional restriction on the authentication response waiting time.

As per Claim 17, the rejection of Claim 16 is incorporated. In addition, Claim 17 is a computer-readable medium claim corresponding to the system claim 2. Thus, it is rejected with the same rationale applied against Claim 2 above.

b. Referring to Claims 7 and 22:

As per Claim 7, Pang et al. disclose an authentication system for authentication:

a processor circuit having a processor and a memory **[Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information. Computer system 100 also includes a main memory 106, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 102 for storing information and instructions to be executed by processor 104 (lines 13-20, Col. 4); where computer system inherently**

***contains circuit board (mother board) for integrating the processor, memory, and other peripheral devices];***

an authentication system stored in the memory and executable by the processor [Fig. 6 is a block diagram of a system 600 that provides for an extensible authentication mechanism in a stateless web environment (lines 59-61, Col. 18 and Fig. 6); ***were the web application server 280 in the system 600 is a type software program and must be stored in the memory to be executed by the processor]***, the authentication system comprising:

a plurality of authentication agents, each of the authentication agents authenticating at least one user parameter by performing at least one authentication task [A plurality of authentication service providers (simply referred to as providers) (lines 1-2, Col. 19). Each provider provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair (lines 26-31, Col. 20). A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from

the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)];

an authentication manager that requests each of the authentication agents to authenticate an unauthenticated user parameter [At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 46-49, Col. 22)]; and

Pang et al. do not expressly disclose wherein, upon startup, the authentication manager is unaware of how many of the authentication agents exist in association with the authentication system and the authentication manger discovers the authentication agents. However, Pang et al. disclose the providers are implemented as dynamically linked libraries (DLLs) and loaded dynamically at the runtime only and the communication of is through the use of Microsoft COM or remote

procedure calls (RPC) **[Providers are implemented as dynamically linked libraries (DLLs). As such, the providers are loaded into and execute within the same address space as the authentication hosts to which they belong (lines 1-4, Col. 20). The providers are preferably loaded dynamically at run time (lines 4-5, Col. 20). For example, the components of web application server 280 may alternatively communicate with each other using Remote Procedure Calls (RPC), a UNIX, Microsoft COM (lines 64-67, Col. 17); where dynamically links at the running time only means the exact number of agents are unknown prior to the process is running]**. Therefore, It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify that Pang et al. to have the discovery procedure of the provider specified since one would be motivated to have a mechanism which allows providers to be dynamically added and removed from the authentication server (lines 22-24, Col. 20 from Pang et al.). Thus, it would have been obvious to modify Pang et al. to obtain the invention as specified in claim 7.

As per Claim 22, it encompasses limitations that are similar to those of Claim 7. Thus, it is rejected with the same rationale applied against Claim 7 above. In addition, Pang et al. disclose a computer program embodied on a computer readable medium for performing authentication



**[The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 104 for execution (lines 58-60, Col. 4)].**

c. Referring to Claim 8:

As per Claim 8, Pang et al. disclose the authentication system of claim 7. Pang et al. do not expressly disclose wherein the authentication manager is configured to generate a lookup table listing each of the authentication agents during the startup after the authentication agents are discovered. However, Pang et al. disclose a function pointer table and a property table maintained in each provider, useful for the authentication host to call the entry pointer to obtain a list of function pointers for authenticating a particular provider request **[(lines 6-17, Col. 20)]** and information of particular provider is stored in the web application server, which contains the authentication host, as metadata when a provider is initialized **[(lines 18-24, Col. 20); where initialization is achieved by the process of dynamically loading at the running time and the record of the dynamically loaded provider is then kept as metadata]**. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Pang et al. to have metadata corresponding to a dynamically loaded provider stored as a table by the authentication host much similar to the fashion as the table of function pointers and properties contained

by the provider since one would have been motivated to conveniently having an authentication host can call the entry point to obtain a list of function pointers that can be used in authenticating a particular provider request (lines 15-17, Col. 20 from Pang et al.). Thus, it would have been obvious to modify Pang et al. to obtain the invention as specified in claim 8.

d. Referring to Claim 14:

As per Claim 14, Pang et al. disclose an authentication method, comprising:

executing a plurality of authentication agents in a computer system **[Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information (lines 13-16, Col. 4). Provider are implemented as dynamically linked libraries (DLL) (lines 1-2, Col. 20); *where the provider is software implemented and must be executed by the computer*]**, each of the authentication agents being configured to perform at least one of the authentication task **[A plurality of authentication service providers (simply referred to as providers) (lines 1-2, Col. 19). Each provider provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only**

those browser request that are associated with a particular username and password pair (lines 26-31, Col. 20). A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)]; and

employing the authentication manager to sequentially request each of the authentication agents to authenticate an unauthenticated user parameter input into the computer system [It shall be assumed that the URL associated with the browser request is associated with the protected string "BASIC(GRUP1) AND IP(IP\_LIST)" and that the browser request contains a username of JIM, a password of "MANAGER" and an IP address of "192.6.25.3" (lines 17-21, Col.

22). At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 45-49, Col. 22); *where manger requests provider 606 to authenticate the first field of the request and the provider 608 to authenticate the second field of the request*];

obtaining a response from each of the authentication agents indicating whether the unauthenticated user parameter has been authenticated [If the BASIC provider finds a username/password match, the BASIC provider sends a message to the authentication host indicating that access should be allowed based on the supplied username and password pair. However, if the BASIC provider does not find a match, the BASIC provider sends a message to the authentication host indicating that access should not be allowed based on the username/password pair (lines 35-42, Col. 20). If the IP address provider finds an IP address match, the IP address provider sends a message to the authentication host indicating that access should be allowed based on the supplied IP address. However, if the IP address provider does not find a match, the IP address provider sends a message to the authentication host indicating that access should not be allowed based on the IP address (lines 50-57, Col. 20)].

Pang et al. do not expressly disclose executing an authentication manager in the computer system, wherein the authentication manager is unaware of how many of the authentication agents exist when the authentication manger is first executed and discovering the authentication agents with the authentication manager upon execution of the authentication manager. However, Pang et al. disclose the providers are implemented as dynamically linked libraries (DLLs) and loaded dynamically at the runtime only and the communication of is through the use of Microsoft COM or remote procedure calls (RPC) **[Providers are implemented as dynamically linked libraries (DLLs). As such, the providers are loaded into and execute within the same address space as the authentication hosts to which they belong (lines 1-4, Col. 20). The providers are preferably loaded dynamically at run time (lines 4-5, Col. 20). For example, the components of web application server 280 may alternatively communicate with each other using Remote Procedure Calls (RPC), a UNIX, Microsoft COM (lines 64-67, Col. 17); *where dynamically links at the running time only means the exact number of providers are unknown prior to the process is running and would link to the providers upon the running time*]**. Therefore, It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify that Pang et al. to have the discovery procedure of the providers by the

authentication host be specified at running time since one would be motivated to have a mechanism which allows providers to be dynamically added and removed from the authentication server (lines 22-24, Col. 20 from Pang et al.). Thus, it would have been obvious to modify Pang et al. to obtain the invention as specified in claim 14.

e. Referring to Claim 15:

As per Claim 15, the rejection of Claim 14 is incorporated. In addition, Claim 15 encompasses limitations that are similar to those of Claim 8. Thus, it is rejected with the same rationale applied against Claim 8 above.

f. Referring to Claim 23:

As per Claim 23, the rejection of Claim 22 is incorporated. In addition, Claim 23 is a computer-readable medium claim corresponding to the system claim 8. Thus, it is rejected with the same rationale applied against Claim 8 above.

8. Claims 4-5, 11-12, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pang et al. (U.S. Patent 6,446,204), and further in view of Stoltz et al. (U.S. Patent 6,615,264).

a. Referring to Claims 4 and 19:

As per Claim 4, Pang et al. disclose a system for authentication comprising:

a processor circuit having a processor and a memory [Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information. Computer system 100 also includes a main memory 106, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 102 for storing information and instructions to be executed by processor 104 (lines 13-20, Col. 4); *where computer system inherently contains circuit board (mother board) for integrating the processor, memory, and other peripheral devices*];

an authentication system stored in the memory and executable by the processor [Fig. 6 is a block diagram of a system 600 that provides for an extensible authentication mechanism in a stateless web environment (lines 59-61, Col. 18 and Fig. 6); *were the web application server 280 in the system 600 is a type software program and must be stored in the memory to be executed by the processor*], the authentication system comprising:

a plurality of authentication agents, each of the authentication agents authenticating at least one user parameter by performing at least one authentication task, wherein a parameter type is associated with each of the authentication agents [A plurality of authentication service providers (simply referred to as providers) (lines 1-2, Col. 19). Each

provider provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair (lines 26-31, Col. 20). A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)],

an authentication manager that requests each of the authentication agents to authenticate an unauthenticated user parameter [At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the



**provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 46-49, Col. 22)]; and**

wherein each of the authentication agents authenticates the unauthenticated user parameter if the unauthenticated user parameter is of the parameter type associated with the respective authentication agent **[A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)]; and**

Pang et al. do not expressly disclose each of the authentication agents transmits a message to the authentication manager that causes the authentication manager to proceed with the authentication procedure if the unauthenticated user parameter is not of the parameter type

associated with the respective authentication agent. However, Stoltz et al. disclose plurality of authentication modules and each has the option of accepting or declining responsibility for a request such that it can accept all the request at all the time, part of the time, or not accepting the request at all and the modules can be cascaded for allowing the authentication process to continue **[Authentication modules 240 each have the option of accepting or declining responsibility for a particular connection. Authentication modules 240 may base their decision on other available system resources or settings (e.g., from services 230-238, external databases, etc.). In one or more embodiments, an authentication module 240 can be configured to accept all users all of the time, to only accept connections with smart cards, or to only accept users with pseudo tokens, for example. In one or more embodiments, authentication modules 240 may be cascaded (lines 57-67, Col. 8); *where declining can be due to the reason, such as the field of authentication is not the right type associated with the module and the authentication process would be continue since modules are cascaded*]**. Pang et al. and Stoltz et al. are analogous art because they are from similar technology relating a system with multiple authentication modules. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Pang et al. with Stoltz et al. to have the

providers with the ability to make a decision on whether to accept or decline a request based on the field type and return the response to the authentication host to allow the authentication process to continue since one would have been motivated to motivated to realize that authentication module makes such decision based on the available system resources or settings (lines 59-60, Col. 8 from Stoltz et al.). Therefore, it would have been obvious to combine Pang et al. and Stoltz et al. to obtain the invention as specified in claim 4.

As per Claim 19, it encompasses limitations that are similar to those of Claim 4. Thus, it is rejected with the same rationale applied against Claim 4 above. In addition, Pang et al. disclose a computer program embodied on a computer readable medium for performing authentication **[The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 104 for execution (lines 58-60, Col. 4)].**

b. Referring to Claims 5 and 20:

As per Claim 5, Pang et al. disclose a system for authentication, comprising:

**[Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information. Computer**

**system 100 also includes a main memory 106, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 102 for storing information and instructions to be executed by processor 104 (lines 13-20, Col. 4); *where computer system inherently contains circuit board (mother board) for integrating the processor, memory, and other peripheral devices*];**

an authentication system stored in the memory and executable by the processor **[Fig. 6 is a block diagram of a system 600 that provides for an extensible authentication mechanism in a stateless web environment (lines 59-61, Col. 18 and Fig. 6); *were the web application server 280 in the system 600 is a type software program and must be stored in the memory to be executed by the processor*], the authentication system comprising:**

an authentication manager that requests each of the authentication agents to authenticate an unauthenticated user parameter **[At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 46-49, Col. 22)];**

wherein each of the authentication agents authenticates the unauthenticated user parameter if the unauthenticated user parameter is of the parameter type associated with the respective authentication

agent [A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)];

wherein:

each of the authentication agents transmits an invalid response to the authentication manager upon a failure to authenticate the unauthenticated user parameter [In this example, the provider request of BASIC(GROUP1)JIM/MANGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (lines 46-49, Col. 22). However, if the BASIC provider does not find a match, the BASIC provider sends a message to the authentication host indicating that access should not be allowed

**based on the username/password pair (lines 35-39, Col. 20). However, if the IP address provider does not find a match the IP address sends a message to the authentication host indicating that access should not be allowed based on the IP address (lines 54-57, Col. 20)];**

each of the authentication agents transmits a valid response to the authentication manager upon a successful authentication of the unauthenticated user parameter [In this example, the provider request of BASIC(GROUP1)JIM/MANGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (lines 46-49, Col. 22). If the BASIC provider finds a username/password match, the BASIC provider sends a message to the authentication host indicating that access should be allowed based on the supplied username and password pair (lines 39-42, Col. 20). If the IP address provider finds an IP address match, the IP address provider sends a message to the authentication host indicating that the access should be allowed based on supplied IP address (lines 50-54, Col. 20)].

Pang et al. do not expressly disclose each of the authentication agents transmits a valid response to the authentication manager if the unauthenticated user parameter is of a parameter type that is different than the parameter type associated with the respective authentication

agent. However, Stoltz et al. disclose plurality of authentication modules and each has the option of accepting or declining responsibility for a request such that it can accept all the request at all the time, part of the time, or not accepting the request at all **[Authentication modules 240 each have the option of accepting or declining responsibility for a particular connection. Authentication modules 240 may base their decision on other available system resources or settings (e.g., from services 230-238, external databases, etc.). In one or more embodiments, an authentication module 240 can be configured to accept all users all of the time, to only accept connections with smart cards, or to only accept users with pseudo tokens, for example (lines 57-65, Col. 8); where declining can be due to the reason, such as the field of authentication is not the right type associated with the module]**. Pang et al. and Stoltz et al. are analogous art because they are from similar technology relating a system with multiple authentication modules. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Pang et al. with Stoltz et al. to have the providers with the ability to make a decision on whether to accept or decline a request based on the field type and return a valid message indicating the request is not of the right type since one would have been motivated to realize that authentication module makes such decision based on the available

system resources or settings (lines 59-60, Col. 8 from Stoltz et al.).  
Therefore, it would have been obvious to combine Pang et al. and Stoltz et al. to obtain the invention as specified in claim 5.

As per Claim 20, it encompasses limitations that are similar to those of Claim 5. Thus, it is rejected with the same rationale applied against Claim 5 above. In addition, Pang et al. disclose a computer program embodied on a computer readable medium for performing authentication **[The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 104 for execution (lines 58-60, Col. 4)].**

c. Referring to Claim 11:

As per Claim 11, Pang et al. disclose an authentication method comprising:  
executing a plurality of authentication agents in a computer system **[Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information (lines 13-16, Col. 4). Provider are implemented as dynamically linked libraries (DLL) (lines 1-2, Col. 20); where the provider is software implemented and must be executed by the computer]**, each of the authentication agents being configured to perform at least one of the authentication task **[A**



plurality of authentication service providers (simply referred to as providers) (lines 1-2, Col. 19). Each provider provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair (lines 26-31, Col. 20). A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)]; and

associating a parameter type with each of the authentication agents, wherein each of the authentication agents authenticates only those

unauthenticated user parameters that are of a parameter type that is associated with the respective authentication agent [At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 46-49, Col. 22)];

sequentially requesting each of the authentication agents to authenticate an unauthenticated user parameter input into the computer system [It shall be assumed that the URL associated with the browser request is associated with the protected string "BASIC(GROUP1) AND IP(IP\_LIST)" and that the browser request contains a username of JIM, a password of "MANAGER" and an IP address of "192.6.25.3" (lines 17-21, Col. 22). At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 45-49, Col. 22); *where provider 606 is authenticating the first field of the request, and the provider 608 is authenticating the second field of the request*];

obtaining a response from at least one of the authentication agents indicating whether the unauthenticated user parameter is of the parameter type associated with the respective authentication agents [At step 718, each provider sends a response message to the

authentication engine 602 via the authentication host 604 (lines 52-54, Col. 22). If the BASIC provider finds a username/password match, the BASIC provider sends a message to the authentication host indicating that access should be allowed based on the supplied username and password pair (lines 39-42, Col. 20). If the IP address provider finds an IP address match, the IP address provider sends a message to the authentication host indicating that the access should be allowed based on supplied IP address (lines 50-54, Col. 20); *where the positive response of the match means the field is of the type associated with the particular provider*]; and

Pang et al. do not expressly disclose obtaining a response from at least one of the authentication agents causing the sequential requesting of the authentication agents to authenticate the unauthenticated user parameter to continue if the unauthenticated user parameter is not of the parameter type associated with the respective authentication agent. However, Stoltz et al. disclose plurality of authentication modules and each has the option of accepting or declining responsibility for a request such that it can accept all the request at all the time, part of the time, or not accepting the request at all, and the modules can be cascaded for allowing the authentication process to continue [Authentication modules 240 each have the option of accepting or declining responsibility for a particular connection. Authentication modules

**240 may base their decision on other available system resources or settings (e.g., from services 230-238, external databases, etc.). In one or more embodiments, an authentication module 240 can be configured to accept all users all of the time, to only accept connections with smart cards, or to only accept users with pseudo tokens, for example In one or more embodiments, authentication modules 240 may be cascaded (lines 57-67, Col. 8); *where declining can be due to the reason, such as the field of authentication is not the right type associated with the module and the authentication process would be continue since modules are cascaded*].** Pang et al. and Stoltz et al. are analogous art because they are from similar technology relating a system with multiple authentication modules. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Pang et al. with Stoltz et al. to have the providers with the ability to make a decision on whether to accept or decline a request based on the field type and return the response to the authentication host to allow the authentication process to continue since one would have been motivated to motivated to realize that authentication module makes such decision based on the available system resources or settings (lines 59-60, Col. 8 from Stoltz et al.). Therefore, it would have been obvious to combine Pang et al. and Stoltz et al. to obtain the invention as specified in claim 11.

d. Referring to Claim 12:

As per Claim 12, Pang et al. disclose an authentication method, comprising:

executing a plurality of authentication agents in a computer system [Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information (lines 13-16, Col. 4). Provider are implemented as dynamically linked libraries (DLL) (lines 1-2, Col. 20); *where the provider is software implemented and must be executed by the computer*], each of the authentication agents being configured to perform at least one of the authentication task [A plurality of authentication service providers (simply referred to as providers) (lines 1-2, Col. 19). Each provider provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair (lines 26-31, Col. 20). A BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser request that are associated with a particular username and password pair. Thus, when the BASIC provider receives a provider request from the

authentication host, the BASIC provider searches a predefined username/password access list to determine if access should be provided (lines 28-35, Col. 20). The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address. Thus, when the IP address provider receives a provider request from the authentication host, the IP address provider searches a predefined IP access list to determine if access should be provided (lines 45-50, Col. 20)]; and

executing an authentication manager in the computer system to sequentially request each of the authentication agents to authenticate an unauthenticated user parameter input into the computer system [Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information (lines 13-16, Col. 4). It shall be assumed that the URL associated with the browser request is associated with the protected string "BASIC(GRUP1) AND IP(IP\_LIST)" and that the browser request contains a username of JIM, a password of "MANAGER" and an IP address of "192.6.25.3" (lines 17-21, Col. 22). At step 714, the authentication host 604 sends the provider requests of (BASIC(GROUP1)JIM/MANAGER is sent to the provider 606 and the

**provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (line 45-49, Col. 22); where manger requests provider 606 to authenticate the first field of the request and the provider 608 to authenticate the second field of the request];**

transmitting an invalid response from at least one of the authentication agents to the authentication manager upon a failure to authenticate a respective user parameter [In this example, the provider request of BASIC(GROUP1)JIM/MANGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the provider 608 (lines 46-49, Col. 22). However, if the BASIC provider does not find a match, the BASIC provider sends a message to the authentication host indicating that access should not be allowed based on the username/password pair (lines 35-39, Col. 20). However, if the IP address provider does not find a match the IP address sends a message to the authentication host indicating that access should not be allowed based on the IP address (lines 54-57, Col. 20)];

transmitting a valid response from at least one of the authentication agents to the authentication manager upon a successful authentication of the unauthenticated user parameter [In this example, the provider request of BASIC(GROUP1)JIM/MANGER is sent to the provider 606 and the provider request of IP(IP\_LIST) 192.6.25.3 is sent to the

**provider 608 (lines 46-49, Col. 22). If the BASIC provider finds a username/password match, the BASIC provider sends a message to the authentication host indicating that access should be allowed based on the supplied username and password pair (lines 39-42, Col. 20). If the IP address provider finds an IP address match, the IP address provider sends a message to the authentication host indicating that the access should be allowed based on supplied IP address (lines 50-54, Col. 20)]; and**

Pang et al. do not expressly disclose transmitting the valid response from at least one of the authentication agents to the authentication manager if the unauthenticated parameter is of a parameter type that is different than the parameter type associated with the respective authentication agent. However, Stoltz et al. disclose plurality of authentication modules and each has the option of accepting or declining responsibility for a request such that it can accept all the request at all the time, part of the time, or not accepting the request at all **[Authentication modules 240 each have the option of accepting or declining responsibility for a particular connection. Authentication modules 240 may base their decision on other available system resources or settings (e.g., from services 230-238, external databases, etc.). In one or more embodiments, an authentication module 240 can be configured to accept all users all of the time, to**



**only accept connections with smart cards, or to only accept users with pseudo tokens, for example (lines 57-65, Col. 8); where declining can be due to the reason, such as the field of authentication is not the right type associated with the module].**

Pang et al. and Stoltz et al. are analogous art because they are from similar technology relating a system with multiple authentication modules. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Pang et al. with Stoltz et al. to have the providers with the ability to make a decision on whether to accept or decline a request based on the field type and return a valid message indicating the request is not of the right type since one would have been motivated to realize that authentication module makes such decision based on the available system resources or settings (lines 59-60, Col. 8 from Stoltz et al.). Therefore, it would have been obvious to combine Pang et al. and Stoltz et al. to obtain the invention as specified in claim 12.

9. Claims 3, 10, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pang et al. (U.S. Patent 6,446,204) as applied to claims 1, 9, and 16 above, and further in view of Paknad (U.S. Pub. 2002/0069247).

- a. Referring to Claim 3:

As per Claim 3, Pang et al. disclose the authentication system of claim 1. Pang et al. do not expressly disclose an external authentication service; and wherein at least one of the authentication agents calls upon the external authentication service to authenticate the unauthenticated user parameter. However, Paknad et al. disclose that external service can be called upon for authentication of the user **[(line 21-24 in [0124])]**. Pang et al. and Paknad et al. are analogous art because they are from similar technology relating to the computer information for user identification. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Pang et al. with Paknad et al. since one would have been motivated to have a system for **creating and managing an electronic network of collaboration sites** (lines 2-3 in **[0005]** from Paknad et al.). Therefore, it would have been obvious to combine Pang et al. and Paknad et al. to obtain the invention as specified in claim 3.

b. Referring to Claim 10:

As per Claim 10, the rejection of Claim 9 is incorporated. In addition, Claim 10 encompasses limitations that are similar to those of Claim 3. Thus, it is rejected with the same rationale applied against Claim 3 above.

c. Referring to Claim 18:

As per Claim 18, the rejection of Claim 16 is incorporated. In addition, Claim 18 is a computer-readable medium claim corresponding to the system claim 3. Thus, it is rejected with the same rationale applied against Claim 3 above.

### **Response to Arguments**

10. Applicant's arguments filed on Oct. 25, 2005 have been fully considered.

- a. Applicant has amended independent claims 1-9, 11-12, and 14-22. In particular, Applicant has changed Claims 4, 5, 7, 11, 12, 14, 19, 20, and 22 from dependent claims to independent claims. This necessitates the new grounds of rejection. Please refer to the rejection above.

### **Conclusion**

11. Applicant's amendment necessitated the new grounds(s) of rejection presented in this Office Action. Accordingly, Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory

period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

- a. Kao et al. (U.S. Patent 6, 651,168) disclose the inventive authentication framework 200 is shown in FIG. 1A in conjunction with several authentication modules providing userid/password authentication 208, smart card authentication 210, and fingerprint authentication 212. The authentication framework 200 is also shown in conjunction with several computer system interfaces, such as the graphical user interface (GUI) 202 and the command line interface (CLI) 206. The invention enables a computer system to authenticate a user with a selected one of a plurality of authentication processes that may be required by a particular target application, such as a banking application or securities trading application. Each of the authentication processes has a distinct sequence of steps and a unique input/output (I/O) interface for exchanging authentication information with the computer system.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F.

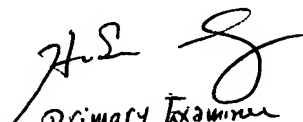
Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Jan. 04, 2006

  
Primary Examiner  
Art Unit 2135